Risk response
- mitigate - put controls in place
- transfer - buy insurance
- avoidance - back out
- deterrence - deter threats
- acceptance - accept risks

Risk concepts
- MTTR - mean time to repair
- MTBF - mean time between failures
- MTTF - mean time to failure
- ALE - annualized loss expectancy
- SLE - single loss expectancy
- ARO - annual rate of occurrence

Risks with cloud computing
- Confidentiality
- Accessibility - downtime?
- Control in other people's hands

Types of firewalls
- Packet filtering - filters every packet
- Application - Layer 7 - allows applications through
- Stateful inspection - if you open a process, let it communicate with you

RTO - recovery time objective - measure of time in which you can recover a device that is down. How long can it be down without giving too much concern?

RPO - recovery point objective - point at which to recover from

VPN - tool used to add security and privacy to networks. An encrypted tunnel

Control types
- Deterrent controls - discouraging potential attackers
- Preventive controls - avoid incident from occurring
- Detective controls - identify incidents or intruders
- Compensating controls - alternative controls
- Technical controls - passwords, smart cards, encryption
- Administrative controls - policies and procedures

Order of volatility
- Registers, cache, RAM
- Network cache, virtual memory
- hard drives, flash drives, CDs, DVDs, and printouts

BIA - business impact analysis

Remove single points of failure!

UPS - uninterruptible power supply

Contingency planning - What if this happens? Do we have backups? etc

Backup frequency
- Normal Backups - backup everything
- Differential backups - files that have changed
- Incremental backups - new files or files that have changed

Archive bit - attribute of a file the OS will use to determine if the file needs to be backed up

Hot site - alternative location where everything is in place
Warm site - alternative location with partial infrastructure
Cold site - alternative location with minimal infrastructure

CIA triad
- Confidentiality - encryption, access controls, steganography
- Integrity - digital signatures, certificates, non-repudiation
- Availability - redundancy, fault tolerance, patching

Types of malware
- Viruses - program that attaches to files. Every time you copy the file, you copy the virus
- Worms - program that replicates itself without any human interaction
- Trojans - program that hides itself in another file
- Rootkits - used to gain administrative privileges
- Backdoors - way for an unauthorized user to access the system
- Logic bombs - piece of malware that activates at a later time
- Botnet - network of compromised computers that are used for purposes such as a DDoS
- Ransomware - encrypts the computer until you pay the attacker
- Polymorphic malware - every time the piece of malware moves places, it changes form
- Armoured virus - designed with encryption so antivirus cannot scan them

Adware - advertising software

Spyware - spying software

Social engineering types
- Phishing - SE via email
- Spim - spam over instant messaging
- Vishing - phishing over telephone/VOIP
- Spearphishing - targeted phishing

Xmas attack - attacker overwhelms your router - DoS on a router

Pharming - corrupting the host files to redirect traffic

DNS poisoning - causes the name server to redirect to the attacker's machine

ARP poisoning - ARP cache is corrupted to redirect traffic

Password attacks
- Brute force attack - guesses password character by character
- Dictionary attack - tries entering passwords from a word list
- Hybrid attack - involve two or more types of attacks to attempt to crack the password
- Birthday attack - used to find collisions in a cryptographic hash function - probability based
- Rainbow tables - precomputed table for reversing cryptographic hash functions

Common attacks
- URL hijacking / typo squatting - an attacker registers a similar domain name to a regular one. Example: I could register googl.com instead of google.com and whoever goes to googl.com goes to my malicious site.
- Watering hole attack - planting malware on reputable sites so you think the software is reputable
- Man in The Middle - attacker places system between you and your intended target
- DDoS - attacker uses a botnet to carry out a DoS attack
- Spoofing - spoofing an IP or MAC address to hide your identity
- Smurf attack - attacker spoofs another PC's address and ping a network to overwhelm the second computer with all the ping replies

Social engineering
- Shoulder surfing - looking over someone's shoulder
- Tailgating - attacker follows an authorized user into a secured building
- Hoax - lying to someone to get them to disclose information
- Phishing - sending deceiving emails to harvest credentials
- Vishing - phishing over telephone/VOIP - phone calls
- Whaling - targeting VIPs such as CEOs or mangers for social engineering
- Spear phishing - targeted phishing
- Dumpster diving - going through trash to find important documents
- Impersonation - pretending to be someone else

Types of wireless attacks
- Rouge access point - AP not authorized to be on you network
    - Evil twin - fake AP to capture credentials
- Jamming - setting up devices to interfere with your signals - DoS
- War driving - driving around searching for open wireless networks
    - War chalking - marking places where there are open wireless networks
- Bluetooth attacks
    - Bluesnarfing - gaining unauthorized access of information from a wireless device through Bluetooth
    - Bluejacking - sending unwanted Bluetooth signals to victims

Application Attacks
- XSS - cross site scripting - enables attackers to inject scripts into webpages view by others
- SQL attack - inject SQL code to run on a database through a web browsing session

XML (extensible markup language) injection - exploit vulnerabilities to inject malicious code held within a database or server
Buffer overflows - direct program execution flow to perform defined tasks by overfilling the buffers.

Zero day exploit - exploit that is not known about. The first time we experience it is the first time it is happening. You can attempt to protect against this by patching and updating your software.

Cookies monitor your web browsing preferences

Session hijacking/ TCP hijacking - attacker gains connection between two parties

Header manipulation - insertion of malicious data into an HTTP response header

Types of logs
- Event logs - let you know what has transpired
- Audit logs - lets you know what is taking place in your networks
- Security logs - who has had access to what
- Access logs - what access was successful, what access was denied

Hardening a system - making a system more secure
- Disable unnecessary services
- Protect management interfaces and applications
- Password protection
- Disable unnecessary accounts

Network security
- MAC filtering - only certain MACs can connect to the network
- MAC limiting - limit number of devices connected
- 802.1x - port based authentication standard
- Disable unused interfaces
- Disable unused application service ports

Increase/decrease signal spread - increase/decrease power level controls

Types of security tools
- Protocol analyzer - capture, filter and display network traffic
- Vulnerability scanner - scans for vulnerabilities on a system
- Honeypot - decoy system that lures attackers into attacking the device so you can study the attack and secure your networks accordingly
- Honeynet - collection of honeypots

Fuzzing - testing your server to see how they respond to errors

Hardware based encryption devices
- TPM - trusted platform module
- HSM - hardware security module
- USB encryption

CIA Triangle
- Confidentiality
- Integrity
- Availability

Kerberos
- KDC - key distribution center - vouches for user's identity
- TGS - ticket granting server - grant you access to resources on the network
- TGT - ticket granting ticket
- SSO - single sign on

Cladding - the glass insulator in fiber optic cabling

Radius - remote authentication dial in user system
- Dial-up user connections
- Facilitates authentication remote users from the outside to an inside network

Kerberos - authentication standard
- Symmetric key cryptography - single sign on
- KDC - key distribution center
- TGS - ticket granting service
- Tickets - used to prevent to replay credentials
- Mutual authentication - user authenticates to the server, and the server authenticates to the user

LDAP - lightweight directory access protocol
- Protocol used to query a database

Access Controls
- Identification - give credentials
- Authentication - verify credentials
- Authorization - check your permissions
- ACLs - access control lists

Access control models
- Mandatory access - security labels
- Discretionary access - owners discretion
- Rule base - set of rules
- Role base - what role you play dictates the permissions you have

SAM - security account manager

Methods of authentication
- Something you know - password
- Something you have - tokens
- Something you are - biometrics
- Somewhere you are - location based authentication
- Something you do - signature dynamics / keyboard dynamics

RC4 is a stream cypher!

Multi-factor authentication MUST include authentication from two different methods!
- Example - Password and token

Cryptography
- Symmetric key - one key used - shared key encryption
- Asymmetric key - two different keys used: public and private key

For communications from Dan to Adam, Dan will use Adam's public key, so that only Adam can decrypt it.

Block cyphers encrypt block by block, stream cyphers encrypt one character at a time

VPN Concentrator - secures all the information entering the VPN

A hashing algorithm that is not collision resistant cannot guarantee integrity

Elliptic curves use a smaller set of keys!

TKIP - temporal key integrity protocol - WPA

PSK - pre sharked key - same key has to be used

Enterprise - user must provide credentials

WEP - RC4
WPA - TKIP
WPA2- CCMP

Hashing
- MD5 - message digest algorithm - used to obscure passwords and insure validity of files - known to be vulnerable
- SHA - secure hashing algorithm
- AES - advanced encryption standard - very fast and very strong

DES - data encryption standard - no longer used
3DES - 3 rounds of computation
HMAC - hashbased message authentication code - the key is never sent
CHAP - challenge handhsake authentication protocol - allows users to securly connect to a system - replaced PAP (password authenticatio protocol)
Onetime pad - combines plain text with random key - used only once

PKI - public key infrastructure
- Symmetric keys - public and private keys
- Registration authority - responisble for verification of the entitiy seeking to achieve a certificate
- Key escrow - trusted 3rd party entity where we keep copies of our keys
- Recovery agent - retrieves the key from the key escrow
- Certificate authority - generates and issues the certificates

DNS zone transfers use TCP port 53